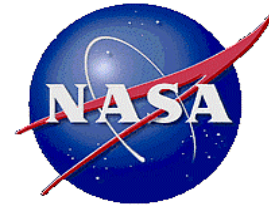


# **Role of System Safety in Risk-informed Decision Making**

**Presented at the  
NASA Risk Management Conference 2005 (RMC VI)  
Orlando, Florida  
December 7, 2005**

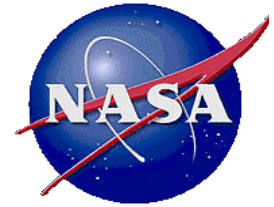
**Homayoon Dezfuli, Ph.D., Manager, System Safety  
Office of Safety and Mission Assurance  
NASA Headquarters**

# System Safety






**System Safety is intended to be a disciplined, systematic approach for the analysis of hazards in order to support decision making aimed at ensuring safety.**

- **“System” is defined as one integrated entity that includes hardware, software, physical environment and human elements**
- **“Safety” is defined as freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.**



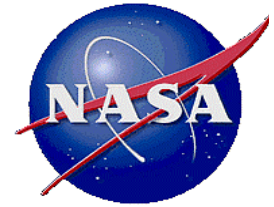
# State-of-Practice Hazards Analysis

- Hazards analysis is the cornerstone of safety assessment
- Hazards analysis is performed using a variety of engineering assessment methods
  - Analyst identifies hazards using modeling techniques such as fault trees, observed hazardous conditions and past occurrences
- Risk matrix is widely used for hazard risk ranking
  - Analyst maps each identified hazard into one of three risk categories using a predefined risk matrix and hazard controls consideration

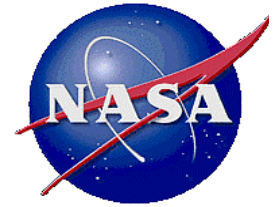
-  Signifies “controlled risk”
-  Signifies “accepted risk”
-  Signifies “unacceptable risk”

Likelihood	Probable			
	Infrequent			
	Remote			
	Improbable			
		Marginal	Critical	Catastrophic
		Severity Levels		

# Limitations of Existing Hazards Analysis Techniques

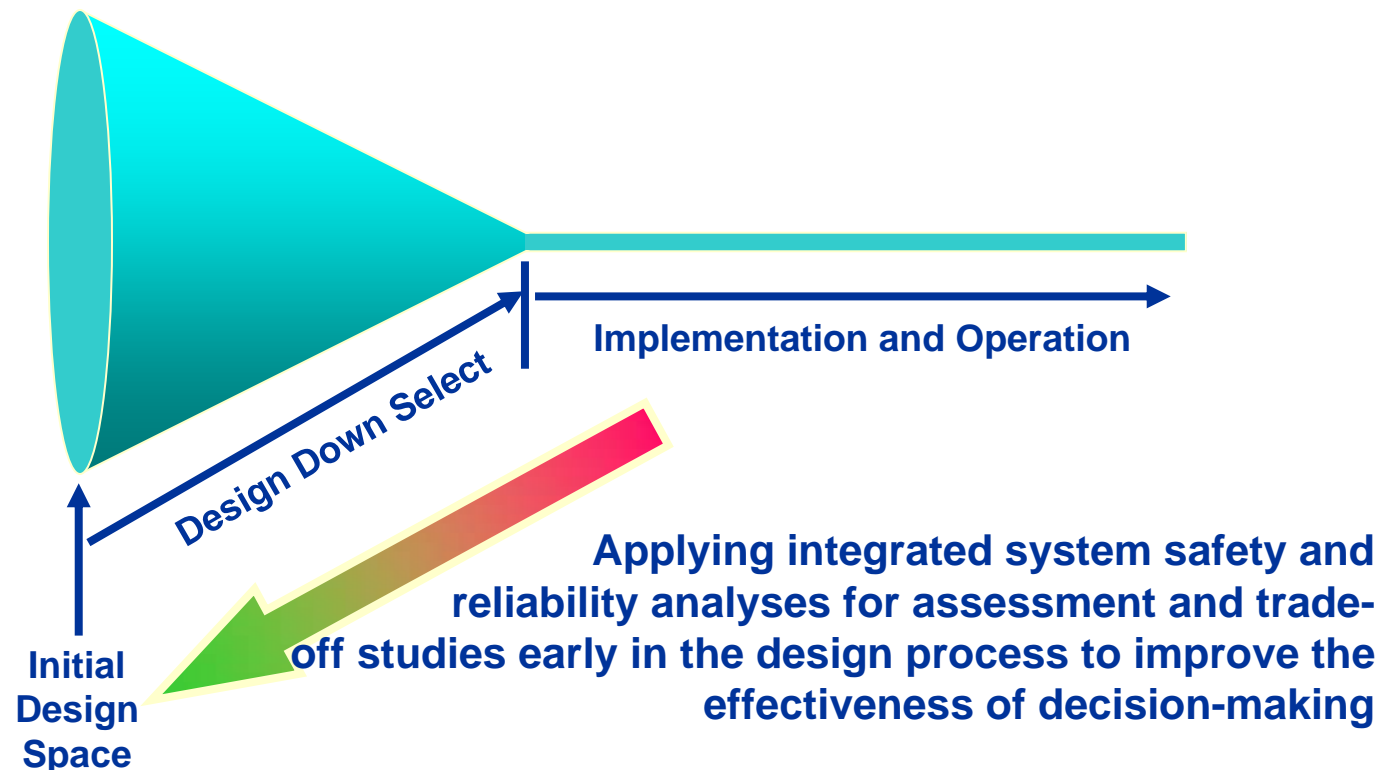


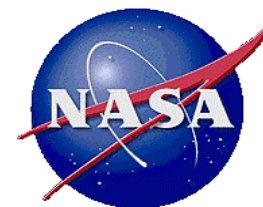
- **Limited ability to affect early design decisions**
  - Typically applied when completed design information is available
  - Typically used as a confirmatory analysis showing low risk for a given hazard
- **Lack of rigor in risk assessment**
  - Risk consequences inappropriately lumped up
  - Ambiguity in the consequence and likelihood scales
  - Too much dependence on known problems
  - Lacks emphasis on the delineation of accident scenarios
  - Interaction between hazards not considered
  - Aggregate risks not obtained
  - Uncertainties not formally accounted for
- **Models not truly integrated (often developed in a stove-pipe manner)**



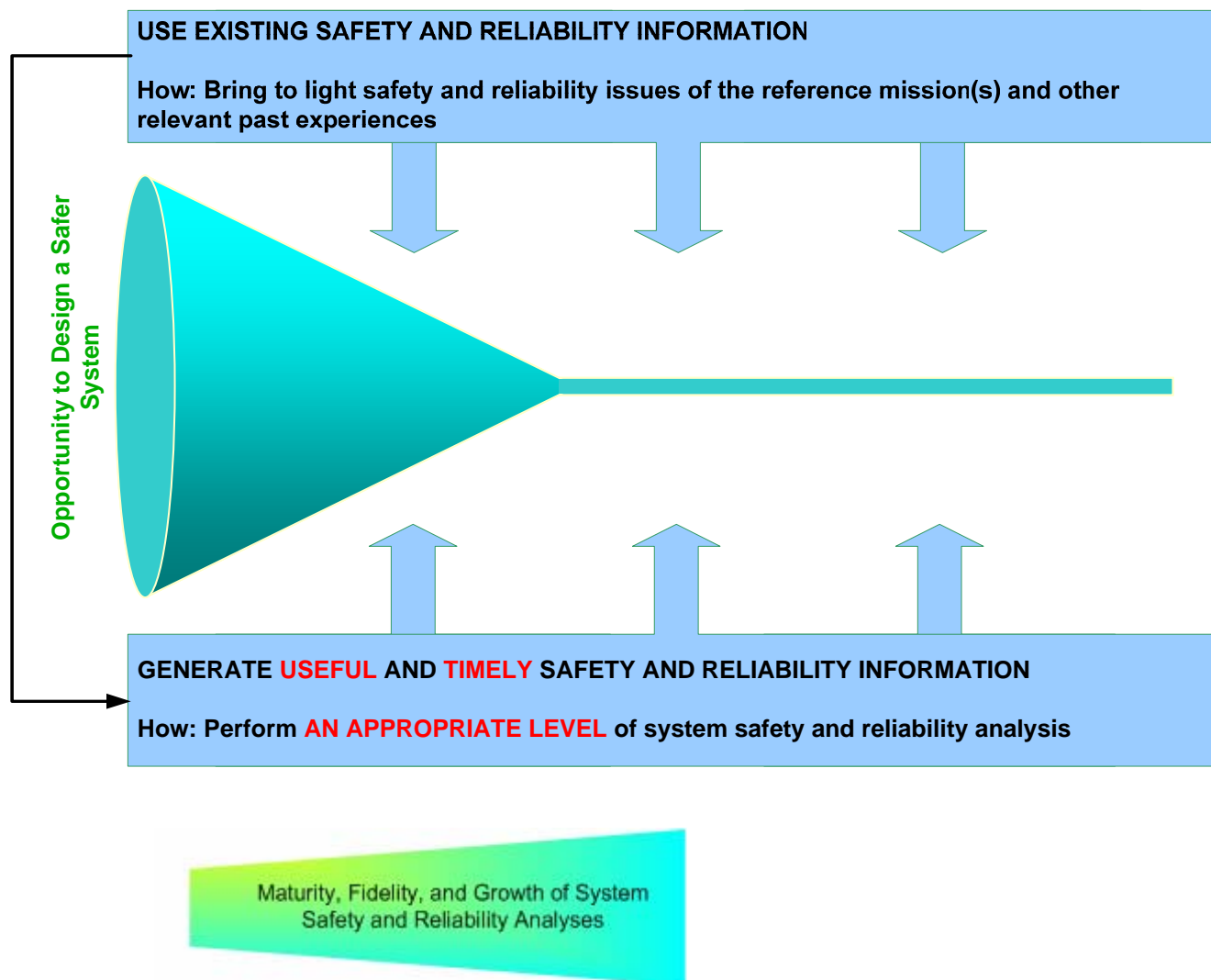
# Reorienting System Safety to Support a Design Environment

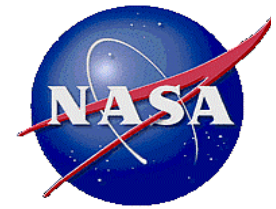
- **FACT:** We are transitioning from the Shuttle Environment to a Design Environment
- **CHALLENGE:** Making system safety activities effective during the design stage





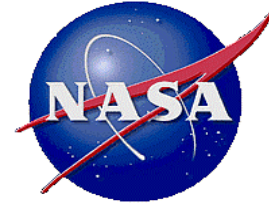
# Timing of System Safety Analyses





# Generation of Useful Safety-related Information

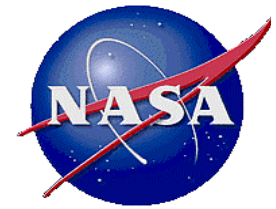
- System safety analysis is essentially an inquiry into how safety adverse consequences could emerge and how to optimally control their risk.
- How do safety adverse consequences emerge?
  - Typically as a result of **accidents**
- What types of Information are needed to enhance safety decisions?
  - Knowledge of **what is important to safety** AND recommendation on what to do about it
  - Knowledge of **what aspects of design or operation are not adequately understood that could potentially impact safety** AND recommendation on how to proceed to gain more knowledge
  - Knowledge of **what is not really important to safety** AND recommendation on ways to take advantage of this opportunity
- What modeling activities should be conducted?
  - Modeling of accidents that have consequences adverse to human life, health, equipment or property, or the environment
  - Assessing risk and uncertainties
  - Formulation of design and operational strategies to control risk
- Risk assessment results are key inputs to risk-informed decision making process
  - Support decisions regarding the acceptability of flight risks
  - Support the allocation of resources for uncertainty and risk reduction



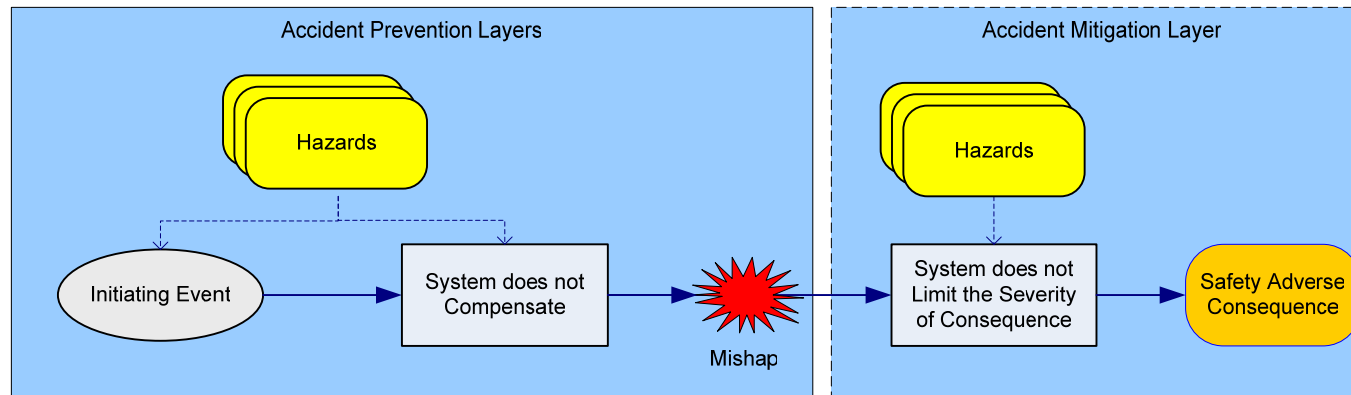
## **A Paradigm Shift in System Safety Analysis is Needed**

- **Adopt a scenario-based accident modeling framework**
  - Analysis of how hazards manifest into accidents
  - Modeling of accident scenarios
  - Integration of different models (e.g., physics-based failure models, fault trees, etc.) into a coherent structure to better delineate accident scenarios
- **Transition from qualitative to quantitative risk assessment**
  - Quantification of risk
  - Recognition and analysis of uncertainties
  - Extending quantitative risk assessment approaches to
    - Developmental phases of system design
    - Mission events evaluation
- **Use of risk information to support decision processes**
  - Treating safety risk as Performance Measures (PMs)
  - Consideration of safety PMs within the trade space



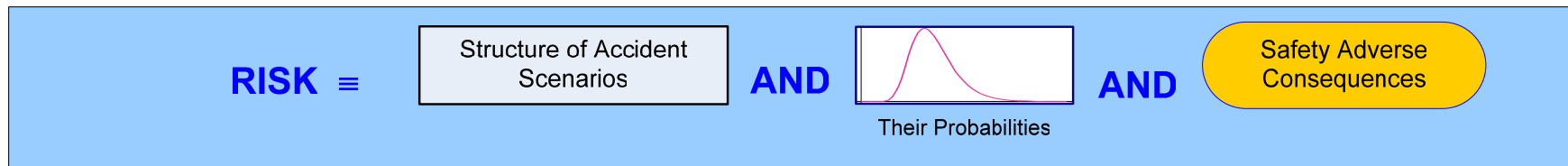
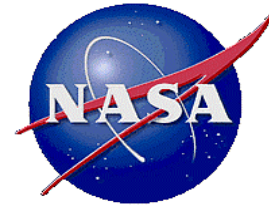


# Adopt a Scenario-based Accident Modeling Framework

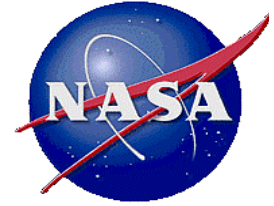


- **A hazard is a state or a set of conditions of a system that together with the occurrence of certain events in the environment of the system could lead to an accident with consequences adverse to safety.**
- **Need for understanding of how a hazard(s) manifests into an accident. Understanding of how it enables or contributes to**
  - the causation of initiating events**
  - the loss of the system's ability to compensate for (or respond to) initiating events**
  - the loss of system's ability to limit the severity of consequences**

# Transition from Qualitative to Quantitative Risk Assessment



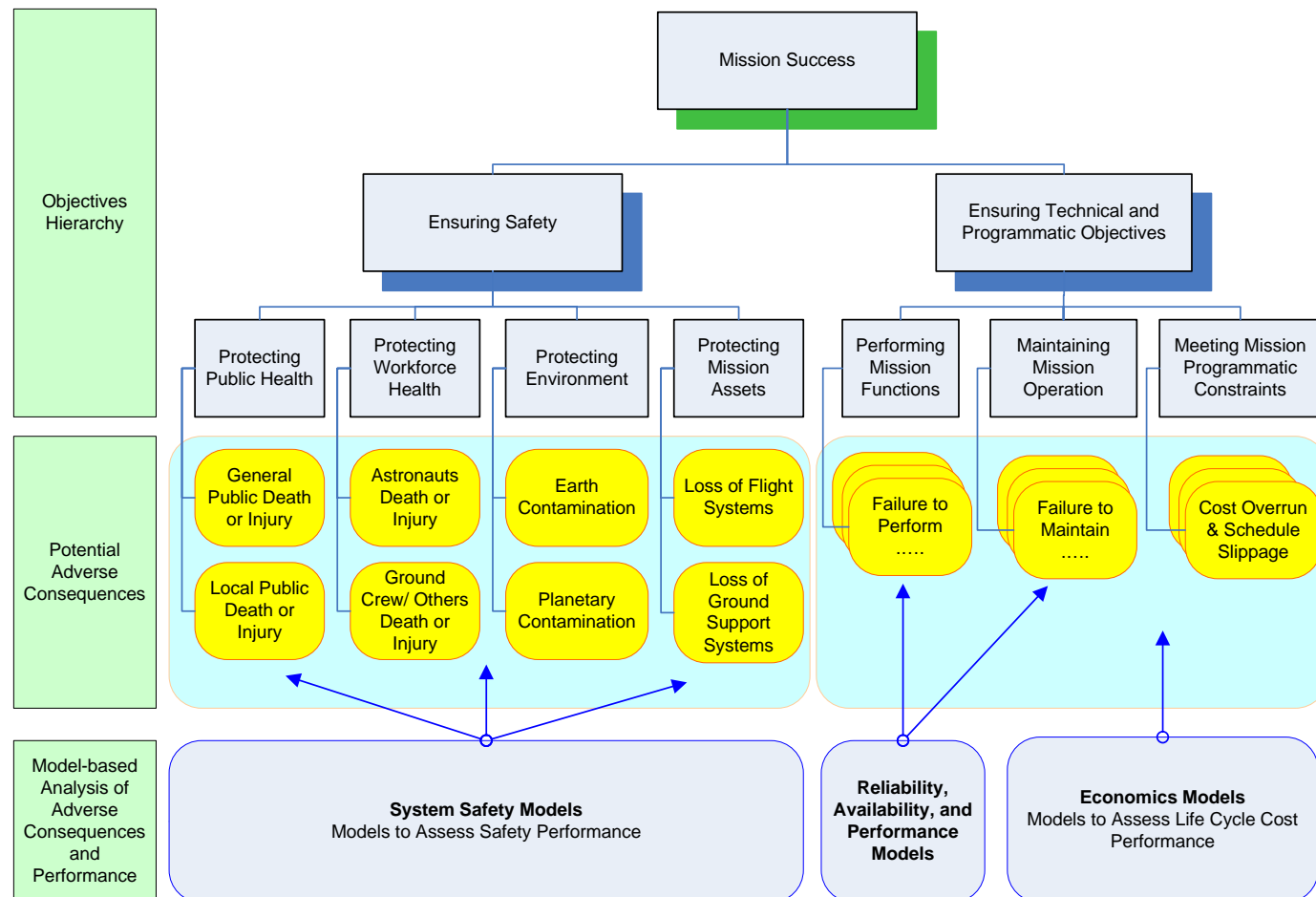
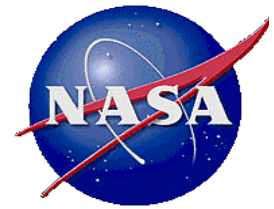
- Treat “risk” as a set of triplets: accident scenarios; associated probabilities and uncertainties; and associated adverse consequences. This interpretation promotes need for ensuring completeness of accident scenario set
- Perform appropriate level of analysis to delineate accident scenarios and to identify dominant risk contributors
- Iterate on risk assessment and continuously re-allocating analytical priorities according to where the dominant risk contributors appear to be coming from
- Structure risk models to allow for trade-off studies
- Assess and quantify uncertainties

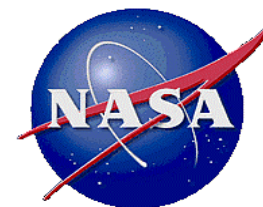


# Risk-informed Performance Measures

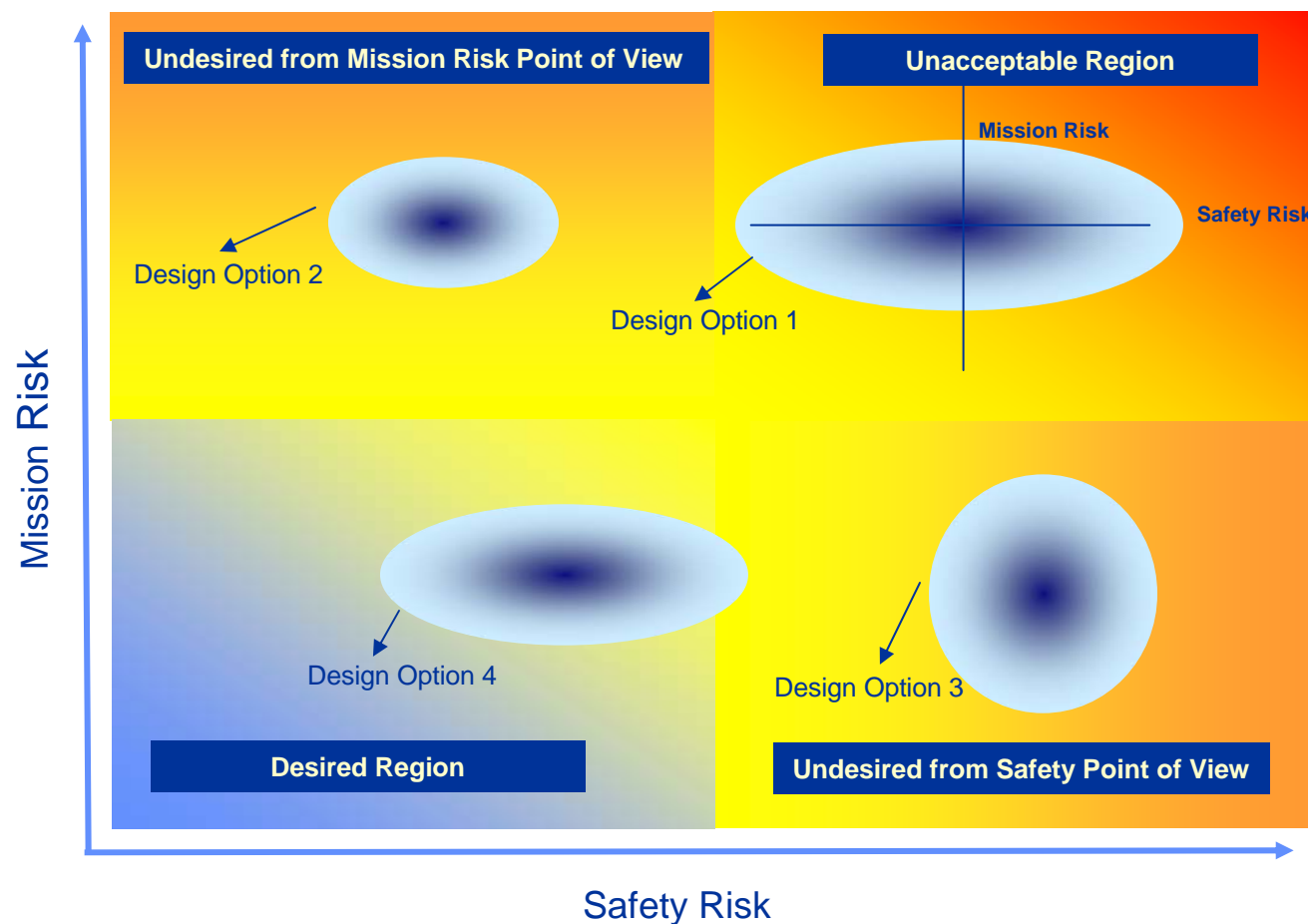
- We are always interested in knowing how our decisions will perform in avoiding safety adverse consequences.
- The "how well" is directly correlated to “how low” the risk of realizing safety adverse consequences are
- Why should we use risk to make a safety case?
  - Because adverse space-related accidents are rare and an absence of accidents doesn't ensure that no accidents will occur in the future
- Risk-informed Performance Measure (PM) is a consequence-oriented metric that is related to risk and/or constituents of risk (e.g., probability).
- Risk-informed Safety PMs are metrics that provide insight into safety performance of a system.
  - Safety PMs provide a means of assessing and monitoring safety performance of a system at different stages of its lifecycle to empower decision processes

# The Role of System Safety and Other Analytical Methods for Risk-informed Decision Making





# Decision Making in the Face of Uncertainties

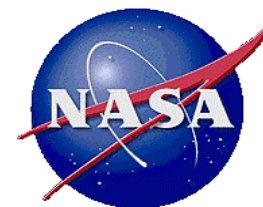


Defining acceptable risk regions specific to the program

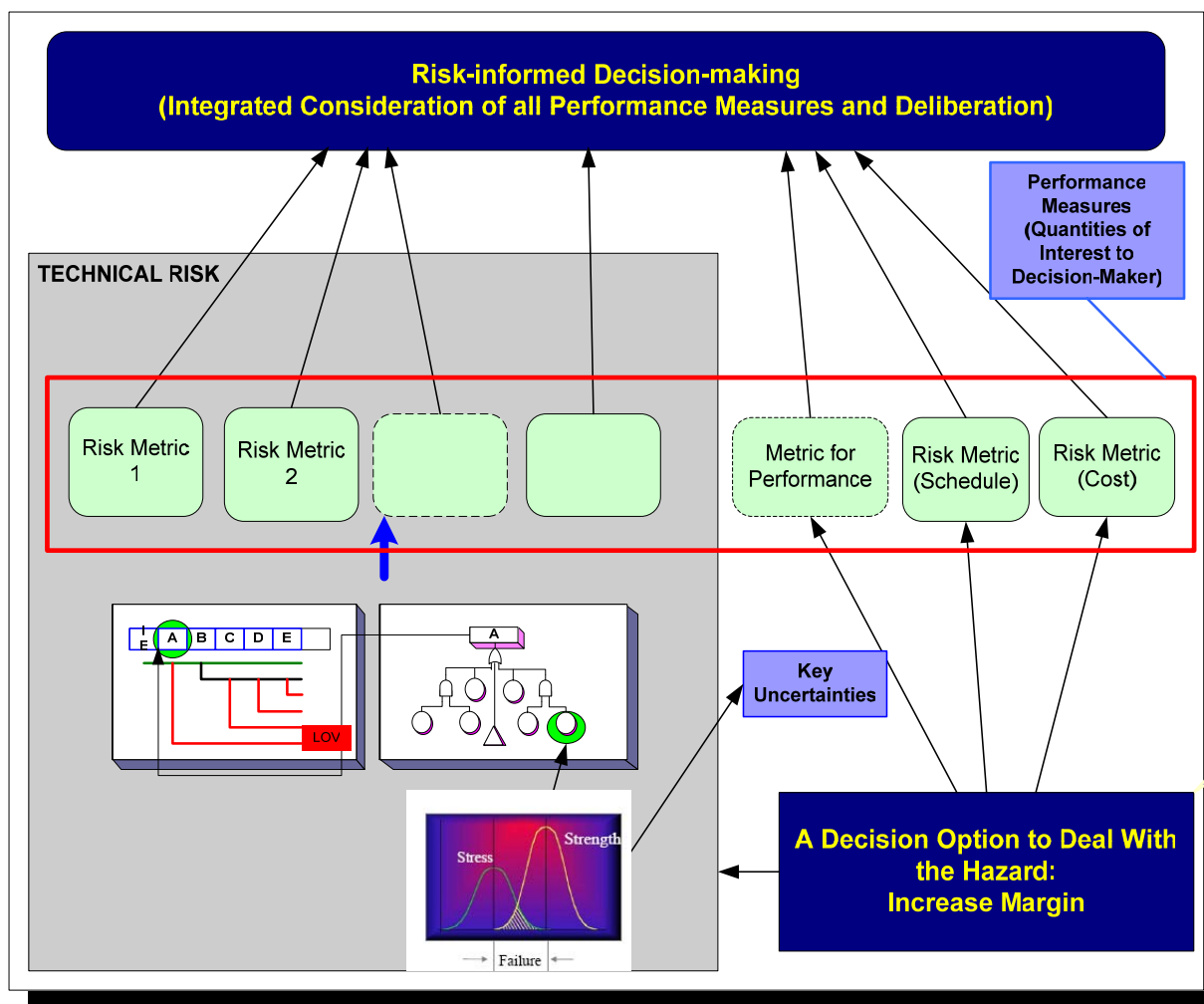
Risk assessment of decision options

Assessment of uncertainties

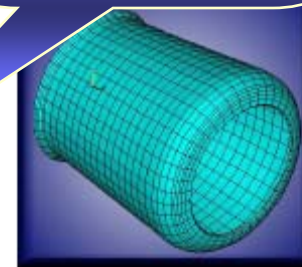
Consideration of risk results including their uncertainties in decision-making



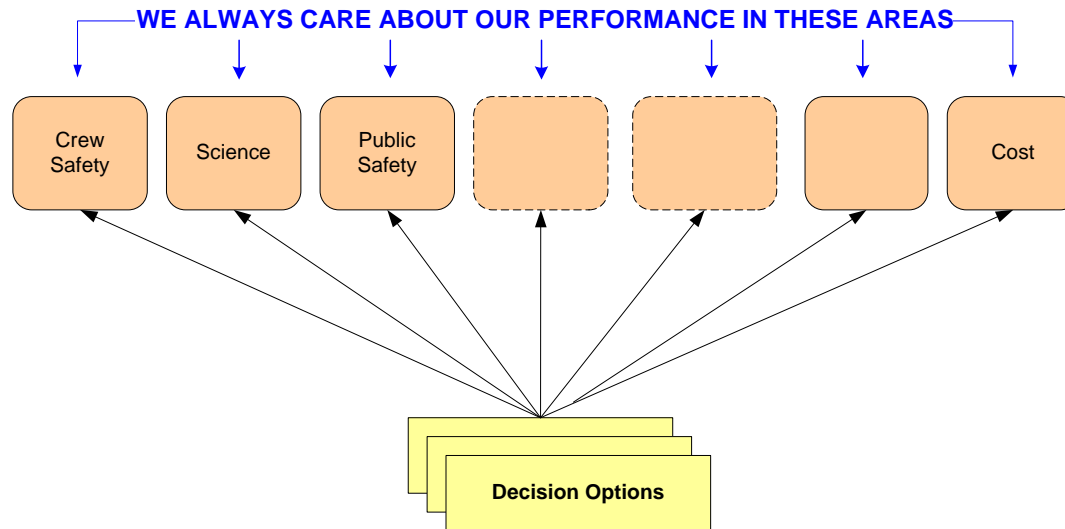
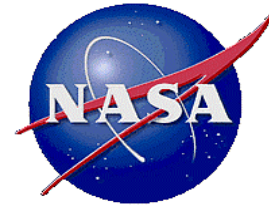
# Risk-informed Analysis of Hazards



**Hazard: Material not strong enough**



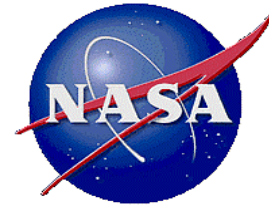
# Need for Engagement of System Safety Analysts in Decision Processes



## Examples of decision situations requiring system safety analyst's involvement

- Designing new systems
- Making changes to existing systems
- Extending the life of existing systems
- Changing requirements
- Responding to operational occurrences in real time
- Allocating resources
- Initiating research programs to reduce uncertainty

# Challenges for Risk-informing System Safety



- Traditional hazard analysis using brainstorming is ingrained into system safety
- System safety analysts organizationally remote from risk analysts
- Shortage of risk analysts
- Recognizing that uncertainties are statements of knowledge
- Overcoming the mindset that quantitative risk assessment requires actuarial (statistical) data
- Lack of structured decision-making processes
- A perception that technical risk assessment is more a database development activity than an analytical activity